(12) UK Patent Application (19) GB (11) 2 262 633 (13) A

(43) Date of A publication 23.06.1993

(21) Application No 9127506.5

(22) Date of filing 31.12.1991

(30) Priority data
(31) 447491 (32) 20.12.1991 (33) IE

(71) Applicant
Uken (Research & Development) Limited

(Incorporated in Ireland)

Gortnafluir, Clonmel, County Tipperary, Ireland

(72) Inventor
Joseph Eustace

(74) Agent and/or Address for Service
Marks & Clerk
57–60 Lincoln's Inn Fields, London, WC2A 3LS,
United Kingdom

(51) INT CL[5]
G06F 12/14

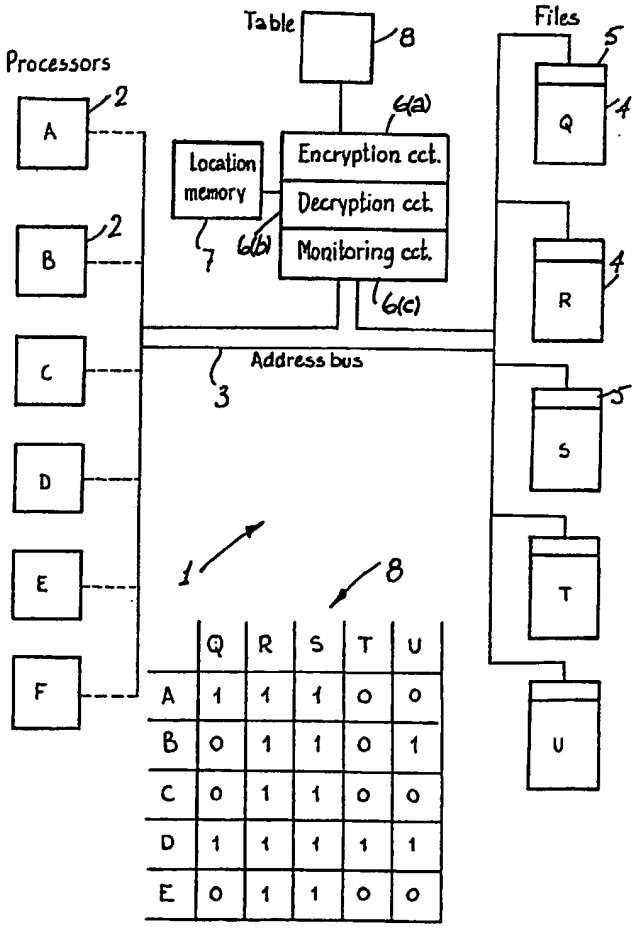
(52) UK CL (Edition L)
G4A AAP

(56) Documents cited
None

(58) Field of search
UK CL (Edition K) G4A AAP
INT CL[5] G06F 12/14

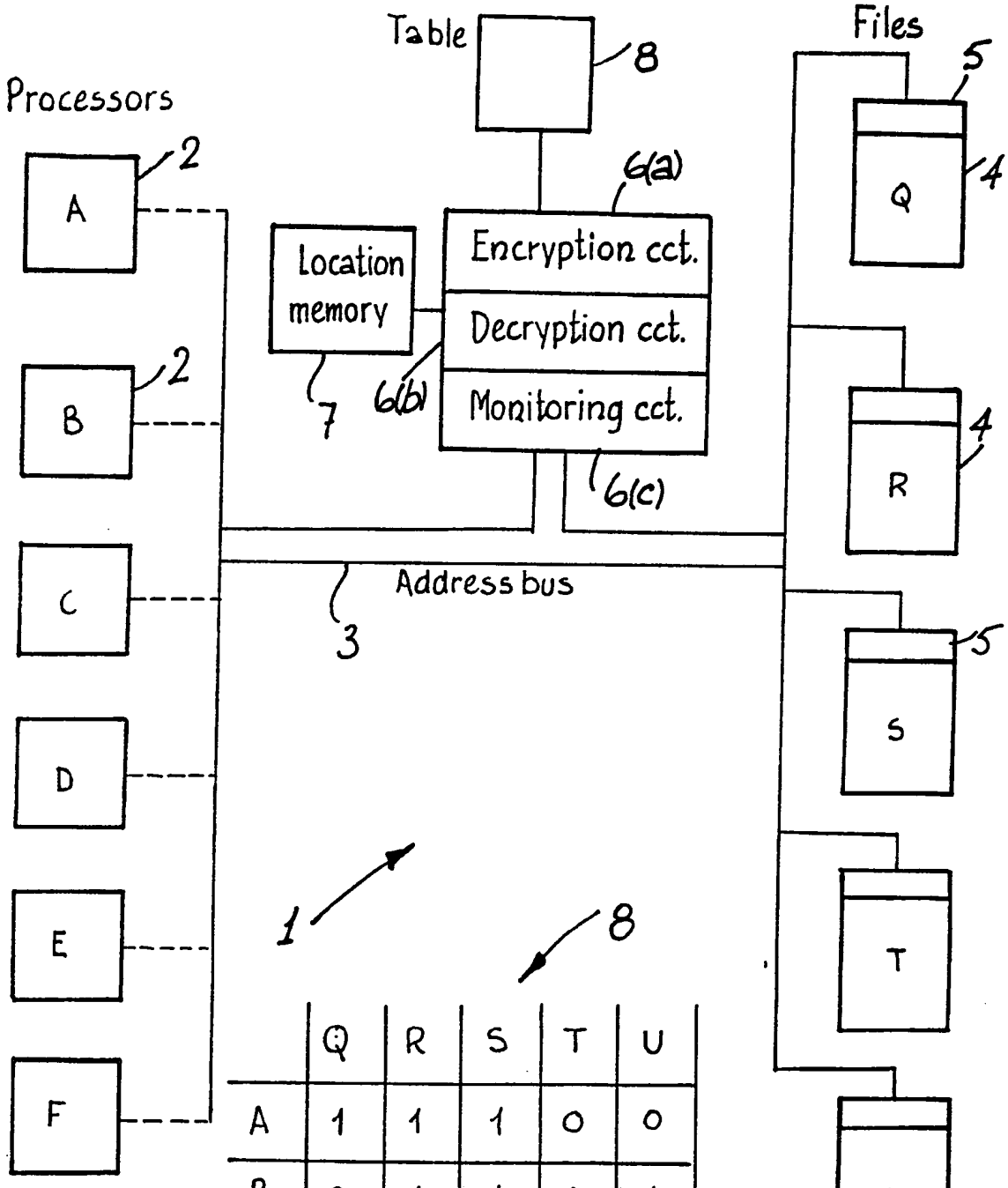
(54) Data security

(57) In a processing apparatus (1) having a number of source processors (2) and stored files (4), a security circuit (6) automatically encrypts the header of files of confidential data when an authorised processor ceases to access the file. Subsequently, if an unauthorised processor attempts to access the confidential file it does not recognise it as a data file and access is not obtained. If an authorised processor attempts to access the confidential file a decryption circuit within the security circuit (6) automatically decrypts the header so that access is obtained. A cross reference table (8) is used to determine which processor may access which files.



	Q	R	S	T	U
A	1	1	1	0	0
B	0	1	1	0	1
C	0	1	1	0	0
D	1	1	1	1	1
E	0	1	1	0	0

GB 2 262 633 A



	Q	R	S	T	U
A	1	1	1	0	0
B	0	1	1	0	1
C	0	1	1	0	0
D	1	1	1	1	1
E	0	1	1	0	0

"Security of Stored Data"

The invention relates to the security of confidential data when stored in a computer system.

It is well known that increasingly widespread storage of data in computer systems leads to an increased risk of access by unauthorised persons to confidential data. For security of transmitted data, enciphering systems such as that described in European Patent Specification No. 166541B1 (Toshiba) and Irish Patent Specification No. 49937 (Interbank) are used. To restrict access to stored confidential data, methods such as those described in British Patent Specification Nos. GB 2195477B (Russel et al) and 2123255B (Marathon) are used whereby access to the data depends on the inputting by a user of a series of temporal information, for example codes and passwords. In a multi-user system, certain circuits which are used for access to "sensitive" or confidential data such as that for personnel, marketing, or payroll may not be used unless password and entry code requirements are met.

The prior art generally relies on preventing operation of certain processors to prevent access to data. However effective such systems may be, they would be ineffective at preventing processors other than those for which password

access is required being used in order to gain access to confidential data. While a person with relatively little skill in computer systems would generally not be able to gain access to confidential data in this manner, skilled persons could instruct different processors to gain access. This is particularly true in computer systems which are interconnected, both in local and wide area networks, in which cases there are many different processors.

The invention is directed towards providing an apparatus which prevents access to confidential data by an unauthorised processor.

According to the invention, there is provided a security apparatus for controlling access of source processors to a confidential data file stored on a storage device, the apparatus comprising:-

a monitoring circuit comprising means for reading storage device address instructions, means for identifying the source processor of an address instruction, and means for identifying the file which is being addressed;

a stored cross-reference table containing authorisation or non-authorisation status indicators for cross-referenced source processors and stored files;

an encryption circuit comprising means for determining from the monitoring circuit and from the cross-reference table when an authorised processor ceases to access a confidential file, and means for subsequently encrypting the header of the confidential file so that it may not be recognised as a data file by any processor;

a decryption circuit comprising means for determining from the monitoring circuit and from the cross-reference table when an authorised source processor is attempting to access a confidential file and means for subsequently decrypting the header so that it may be accessed by the source processor.

The invention will be more clearly understood from the following description of some preferred embodiments thereof, given by way of example only with reference to the accompanying drawing which shows a security apparatus of the invention connected in a computer system.

Referring to the drawing, there is illustrated portion of a computer system 1 to which several different processors 2 identified by the letters A to F may be connected in an address bus 3. The address bus 3 is connected to a fixed disk drive, on the disks of which are stored a number of files indicated generally by the numeral 4 and specifically by the

letters Q to U. Each of the files 4 has a header 5 which is used for identification of the file by the processors 2.

In addition, there is illustrated a security apparatus including a security circuit 6 which is connected to the address bus 3. The security circuit 6 includes an encryption circuit 6(a), a decryption circuit 6(b), and a monitoring circuit 6(c), which are described in more detail below. The security circuit 6 is connected to a location memory 7 which stores the location of all of the files 4. A cross-reference table 8 is also connected to the security circuit 6. This stores access authorisation status indicators for all the processors 2 cross-referenced with the files 4. For example, if file T contains confidential data, the table 8 would store a status indicator which indicates that only processor D may access file T. At the same time, the table may indicate that all processors A to F may access file S. Such a table is illustrated in the drawing in which indicators "1" are used to show that access is authorised and "0" to show that access is not authorised. It will be seen from the table 8 that the processor E has restricted access to the files as files S and R are the only ones which may be accessed, whereas the processor D is authorised to access all of the files. In practice, the processor D would have a complex security system to restrict use of the processor.

The monitoring circuit 6(c) is constructed to continuously monitor the address bus 3 and read addressing instructions for the files 4. The monitoring circuit is also constructed to identify the source processor of an address instruction and to identify from the address instruction the file to which access is sought.

The encryption circuit 6(a) is connected to both the monitoring circuit 6(c) and to the cross-reference table 8 and is constructed to determine when an authorised processor 2 ceases to access a confidential file 5. For example, it may determine when processor D is finished accessing file Q, which contains confidential data. When access is finished, the encryption circuit 6(a) transmits signals on the address bus 3 and encrypts the header 5 of the file so that it may not be recognised by any processor as a data file. Thus, without exception, any processor which attempts to obtain access to that file will not succeed in doing so because it will not be recognised as a data file. This includes not only the normally used processors 2, but also any additional processor connected to the bus 3. The important point is that details of the processor need not be stored in the table 8 to prevent retrieval of confidential files.

The decryption circuit 6(b) continuously operates to monitor address instructions for the files. If access is being attempted to a file for which access is not authorised by at

least one of the processors (i.e. files Q, T and U), the source processor of the instruction is identified and a fetch cycle is made to the cross-reference table 8 to determine if that processor is authorised access to the file. If not, the encryption circuit does not do anything and the processor will not access the file because the header is encrypted. However, if the source processor is authorised, the decryption circuit will immediately decrypt the file header so that access is obtained. It will be appreciated that because the decryption circuit does not need to carry out any action unless the processor is positively authorised, the chances of an unauthorised processor gaining access because of a fault in the security circuit are avoided. If the decryption circuit is inactive for some reason, the worst that can happen is that authorised processors will not gain access. In such circumstances, it is envisaged that back-up files will be stored which will be accessible to only a limited number of personnel who could use these for access to the data.

The invention operates on the principle that all files for which there is confidentiality regarding at least one of the processors may not be accessed unless a positive action is taken by the security apparatus. This is important for maintaining confidentiality of personnel or marketing information. It will also be appreciated that the invention is extremely simple in operation, and relatively simple and

readily available circuits such as monitoring and encryption circuits are required for it's implementation.

The invention is not limited to the embodiments hereinbefore described, but may be varied in construction and detail.

CLAIMS

1. A security apparatus for controlling access of source processors to a confidential data file stored on a storage device, the apparatus comprising:-

a monitoring circuit comprising means for reading storage device address instructions, means for identifying the source processor of an address instruction, and means for identifying the file which is being addressed;

a stored cross-reference table containing authorisation or non-authorisation status indicators for cross-referenced source processors and stored files;

an encryption circuit comprising means for determining from the monitoring circuit and from the cross-reference table when an authorised processor ceases to access a confidential file, and means for subsequently encrypting the header of the confidential file so that it may not be recognised as a data file by any processor;

a decryption circuit comprising means for determining from the monitoring circuit and from the

cross-reference table when an authorised source processor is attempting to access a confidential file and means for subsequently decrypting the header so that it may be accessed by the source processor.

2. An apparatus substantially as hereinbefore described with reference to and as illustrated in the accompanying drawing.

Patents Act 1977
Examiner's report to the Comptroller under Section 17 (The Search Report)

Application number

9127506.5

Relevant Technical fields

(i) UK Cl (Edition K) G4A (AAP)

(ii) Int Cl (Edition 5) G06F (12/14)

Search Examiner

S J PROBERT

Databases (see over)

(i) UK Patent Office

(ii)

Date of Search

19 MARCH 1992

Documents considered relevant following a search in respect of claims 1-2

Category (see over)	Identity of document and relevant passages	Relevant to claim(s)
	NONE	

Category	Identity of document and relevant passages	Relevant to claim(s)

Categories of documents

X: Document indicating lack of novelty or of inventive step.

Y: Document indicating lack of inventive step if combined with one or more other documents of the same category.

A: Document indicating technological background and/or state of the art.

P: Document published on or after the declared priority date but before the filing date of the present application.

E: Patent document published on or after, but with priority date earlier than, the filing date of the present application.

&: Member of the same patent family, corresponding document.

Databases: The UK Patent Office database comprises classified collections of GB, EP, WO and US patent specifications as outlined periodically in the Official Journal (Patents). The on-line databases considered for search are also listed periodically in the Official Journal (Patents).

Published 1993 at The Patent Office, Concept House, Cardiff Road, Newport, Gwent NP9 1RH. Further copies may be obtained from Sales Branch, Unit 6, Nine Mile Point, Cwmfelinfach, Cross Keys, Newport, NP1 7HZ. Printed by Multiplex techniques ltd, St Mary Cray, Kent.